안전하고 효율적인 동적 멀티캐스트 키 관리 구조 제안

박희운[†] · 이임영[††]

요 약

통신 및 컴퓨터의 보급 발전을 통해 공개 네트워크 상에서 그룹에 기반한 통신 응용 서비스의 요구가 증가하고 있다. 이러한 필요성에 따라 멀티캐스트 기반 구조에 대한 연구가 활발히 진행되고 있다. 하지만 멀티캐스트 구조에 대한 안전성과 효율성 및 확장성 부분에 대한 해결책은 아직 미비한 상태이다. 본 연구에서는 기존의 대표적인 멀티캐스트 키 관리 구조를 고찰함과 동시에 안전성과 효율성 및 확장성을 분석한다. 이에 기초해 확장성을 제공하는 안전하고 효율적인 멀티캐스트 키 관리 구조를 제안하고, 기존 방식과 통신 및 계산량 부분에 비교 분석을 통해 그 효율성을 확인한다.

A Proposal of Secure and Efficient Dynamic Multicast Key Management Structure

Hee-Un Park[†] and Im-Yeong Lee[††]

ABSTRACT

With the rapid expansion of computer applications and digital communication networks, group based applications on the open network have been common tendency. The multicast infrastructure has played an important researching part in this application area. However the conventional solutions to achieve the secure and efficient multicast structure don't satisfy all requirements. In this study, we classified and analyzed several existing multicast key management structure on the safety, the efficiency and the strengthen. Based on the analysis, we developed a new secure and efficient multicast key management structure. By comparing various aspects, that the number of communication and computation, of the new and the conventional methods, we were able to demonstrate the effectiveness of the proposed method.

1. 서 론

컴퓨터의 보급 확산과 공용 네트워크의 발전을 통해 세계 곳곳의 정보를 한눈에 볼 수 있는 시대가 도래하고 있다. 이러한 상황에서 사용자들은 단순한 통신에서 벗어나 다자간 통신 회의 및 의료 분야에서 원격 진단 및 상담 등 다양한 서비스를 요구하고 있다. 그러나 이와 같은 서비스는 기존의 일대일 통신 방식으로는 제약 사항이 생길 수밖에 없다. 이를 해결하기 위하여 현재 각광을 받고 있는 방식 중의 하나가 멀티캐스트 기법이다[8-14].

멀티캐스트란 그룹에 참가한 멤버들 사이에서 한 송신자로부터 다수의 참여자에게 메시지 전송이 가능한 방법을 의미한다. 이때 그룹 멤버가 해당 그룹을 떠나면 더 이상 정보를 수신할 수 없게 된다. 동시에 멀티캐스트 기법은 기존의 통신 방식에 대해 그룹에 참가한 송신자의 전송 오버헤드, 네트워크 대역폭 및 지연을 감소시키는 장점을 제공한다.

그러나 멀티캐스트 서비스는 인터넷과 같은 공개된 네트워크를 이용하므로 많은 부분에서 안전성에 대한 취약성이 노출되고 있다. 특히 불법적인 제 3자

본 연구는 정보통신부의 ITRC 사업에 의해 수행된 것임
[†]준회원, 순천향대학교 전산학전공 박사과정
[††]정회원, 순천향대학교 정보기술공학부 부교수

의 도청이나 전송 정보의 위조는 그 대표적인 예가 된다.

이러한 불법 행위로부터 안전성과 신뢰성을 확보하기 위해 암호 시스템이 이용되고 있다. 그러나 키의 노출 여부는 전송 정보의 안전성과 직결되므로 매우 중요시 다뤄져야 한다. 동시에 회원의 가입 및 탈퇴를 위하여 확장성이 보장되어야 한다.

현재 멀티캐스트 그룹 키 관리 분야와 관련하여, 그 중요성에도 불구하고 해결책들은 미흡한 상황이다. 따라서 본 연구는 향후 광범위하게 적용될 멀티캐스트 서비스에서 신뢰성 및 확장성을 제공하기 위하여 요구되는 사항들을 고려한다. 또한, 기존의 멀티캐스트 키 관리 구조들을 고찰함과 동시에 새로운 방식을 제안하여 안전성, 효율성 및 확장성 부분에서 비교 분석을 수행한다.

2. 멀티캐스트 키 관리 요구사항

멀티캐스트 구조는 그 특성상 다자간 통신을 전제로 하고 있기 때문에 여러 위협 요소에 노출되어 있다. 특히 통신을 위해 사용되는 키의 관리는 매우 중요한 요소로서, 다음은 이를 위해 요구되는 사항을 기술한 것이다.

- 무결성 : 멀티캐스트 정보는 전송 도중에 불법적인 제 3자로부터 위조 및 변경되어서는 안된다.
- 인증성 : 송ㆍ수신된 멀티캐스트 정보가 불법적인 변조 없이 정당한 참여자들로부터 생성 및 수신되었음을 확인할 수 있어야 한다.
- 접근 제어 : 정당한 그룹의 소속원만이 멀티캐스트 정보에 접근할 수 있다.
- 부인 봉쇄 : 멀티캐스트 서비스 참여자 사이에서 전송 및 수신 사실을 부인할지라도 당사자 및 제 3자가 이를 확인 할 수 있어야 한다.
- 비밀성 : 불법적인 제 3자로부터 멀티캐스트 정보는 보호되어야 한다. 이를 위해 다양한 암호 기법이 적용될 수 있다.
- 공정성 : 멀티캐스트에서 사용되는 키들은 허가된 그룹 참여자에게만 안전하게 전송되어야 한다. 또한 가입 및 탈퇴를 대비해 키 갱신 프로토콜은 필수적이다. 이를 위해 서버의 독단이나 제 3자와의 불법적 결탁을 방어하기 위한 수단이 확보되어야 한다.
- 확장성 : 멀티캐스트 서비스는 다자간 통신을 전제로 하므로 그룹 참여자의 변동이 생기게된다. 따라서 참여자 변동에 따른 동적인 키 관리 기법이 필요하다.

3. 그룹 키 분배 방식 분석

본 장에서는 기존에 제안된 몇몇 대표적인 그룹 키 분배 방식들의 특징들을 살펴보고, 이 방식들을 멀티캐스트 키 관리 방식에 적용했을 경우 효율성 비교 분석에 이용한다.

3.1 Diffie-Hellman(DH)방식

이 방식은 양자간 통신 키 분배를 위해 1976년에 Diffe-Hellman에 의해 제안된 방식이다[1]. 이 방식은 셋이나 그 이상으로 쉽게 확장이 가능하며, 별도의 키 생성 기관은 필요 없지만 프로토콜 상에서 제 3자에 의한 man-in the-middle attack이 허용된다. 이는 키의 출처를 확인할 방법이 없기 때문에 발생된 문제이다. 또한, 키 생성 과정에서 각각의 가입자들 사이에 하나씩의 공통키를 생성해야 하므로, n명의 가입자에 대해 ${}_nC_2$개의 키가 필요하다. 따라서 통신 회수는 회의 참여자의 수에 의존하는 단점을 가지고 있다.

3.2 Ingemarsson-Tang-Wong(ITW)방식

본 방식은 n명의 가입자들 사이에 하나의 비밀 통신키를 생성하는 방식으로 이산 대수의 어려움에 근거하고 있으며, 원형 및 Ring형 네트워크 구조상에서 이용 가능한 키 분배 기법을 보여주고 있다[2]. 이 방식은 각 가입자로부터 온 전송 정보가 정당한 사용자로부터 온 것인지 판단할 근거가 없다는 문제점을 가지고 있지만, 통신 회수를 3회로 줄임으로서 효율성을 높이고 있다.

3.3 Koyama-Ohta(KO)방식

이 방식은 ID에 기반한 공개키 암호 방식을 이용하여 메시지 인증이 가능한 그룹 키 분배 방식이다[3]. 원형, 성형 및 완전 그래프 네트워크에서 실행 가능하며, 그룹 참가자 모두가 Smart 카드를 이용한다는 특징을 가지고 있다. 본 방식은 이산 대수의 어

려움에 근거한 방식으로 제 3자의 불법 행위를 방지하기 위해 인증성을 제공하고 있기는 하지만, 완벽하지는 않다. 즉, 네트워크 상의 불법 행위자에 의해 양방향 위장 공격이 수행될 경우 정확한 키를 제공하지 못할 수도 있다.

3.4 Burmester-Desmedt(BD)방식

이 방식은 이산 대수에 근거한 공개키 암호 시스템에 기반을 둔 방식으로 사용자 인증 및 그룹 키 계산이 가능한 방식이다[4]. 또한 가입자 수와는 무관한 통신 회수를 갖는 장점과 완벽한 인증성을 제공함으로서 제 3자의 불법적 행위를 막고 있다. 그러나, 인증을 위해서는 모든 가입자들의 공개키를 가지고 있어야 한다는 문제점을 가지고 있으며, 키 분배 과정과 인증 과정이 별도로 수행됨으로서 비효율적인 측면을 가지고 있다. 뿐만 아니라, 통신 회수 역시 키 분배 및 인증을 위해 4회 이상 요구되므로 문제점을 드러내고 있다.

3.5 Park-Lee(PL)방식

본 방식은 ID에 기반한 공개키 암호 시스템에 근거한다[5-7]. 기존의 방식에 비하여 각 참여자는 키 인증 부분과 Bridge를 통해 안전성을 확보하고 있다. 또한 키 생성 시, 2번 정도의 통신 회수를 요구함으로서 효율성을 높이고 있다. 특히 비밀 정보 생성을 위해 참여하는 TC(Trusted Center)는 키 생성에 별도로 참여하지 않음으로서, 부정의 소지를 막고 있다. 각 참여자들과 Bridge가 인증을 통해 해쉬된 신원정보를 확인할 수 있게 함으로서 제 3자의 불법적 행위를 방지할 수 있으며, TC가 키 생성에 참여하지 않으므로 신뢰성을 높일 수 있는 방안이다. 또한, Bridge를 도입함으로서 중간 단계의 안전성을 확보할 뿐만 아니라, 참여자들의 총 라운드 수를 2회로 줄임으로서 효율성을 확보하고 있다.

4. 멀티캐스트 키 관리 구조 분석

4.1 Clique 방식

이 방식은 Diffee-Hellman 방식을 이용하여 그룹 내에 같은 속성을 갖는 소규모 그룹을 구성하는 방식이다[8,9].

4.1.1 프로토콜

1) 시스템 계수

- n, m : 각 그룹 멤버들의 수
- i, j, k, p : 그룹 멤버의 색인
- MBR_i : i번째 그룹 멤버
- g : 밑수
- N_i : MBR_i에 의해 생성된 랜덤 승수
- S, T : $\{N_1, .., N_n\}$의 부분 집합
- $\Pi(S)$: S상의 모든 요소들의 곱
- K_n : n명의 멤버들에게 나눠진 그룹 키

2) 그룹 초기 키 동의 과정

그룹 초기 키 동의는 다음과 같다.

- $MBR_i \rightarrow MBR_{i+1}$: $\{g^{((N1...Ni)/Nk)} \mid k \in [1, i]\}$, $g^{N1...Ni}$
- $MBR_n \rightarrow MBR_i$: $\{g^{((N1...Nn)/Ni)} \mid i \in [1, n]\}$

3) 멤버 가입

멤버 가입의 경우에는 다음과 같은 일을 수행한다. 본 방식은 버스형 네트워크 또는 링(Ring)형 구조에 적합하도록 구성되어 있기 때문에 키 동의시 누가 마지막으로 키 동의에 참여하느냐에 따라 동적 또는 정적으로 구분된다.

가) 동적 그룹 제어

- $MBR_n \rightarrow MBR_{n+1}$: $\{g^{((N1...Nn)/Nk)} \mid k \in [1, n]\}$, $g^{N1...Nn}$
- $MBR_{n+1} \rightarrow MBR_i$: $\{g^{((N1...NnNn+1)/Ni)} \mid i \in [1, n]\}$

나) 정적 그룹 제어

- $MBR_{n+1} \rightarrow MBR_n$: $\{g^{((N1...Nn-1)/Ni)} \mid i \in [1, n-1]\}$, $g^{N1...Nn-1}$
- $MBR_n \rightarrow MBR_{n+1}$: $\{g^{((N1...Nn)/Ni)} \mid i \in [1, n]\}$, $g^{N1...Nn}$
- $MBR_{n+1} \rightarrow MBR_i$: $\{g^{((N1...Nn+1)/Ni)} \mid i \in [1, n]\}$

4) 기존 타 그룹의 멤버 가입

- $MBR_{n+j} \rightarrow MBR_{n+j+1}$: $\{g^{((N1...Nn+j)/Nk)} \mid k \in [1, n+j]\}$, $g^{N1...NnNn+1...Nn+j}$
- $MBR_{n+m} \rightarrow MBR_i$: $\{g^{((N1...Nn+m)/Ni)} \mid i \in [1, n+m]\}$

5) 그룹 탈퇴

- $MBR_n \rightarrow MBR_i$: $\{g^{((N1...Nn)/Ni)} \mid i \in [1, n-1] \wedge i$

≠p} (단, p는 탈퇴 멤버 색인)

4.1.2 특 징

이 방식은 버스형 또는 링(Ring) 형 네트워크 구조에서 적용 가능한 기법이다. 키 분배를 위해서 각 멤버는 공개키 방식에 기반한 Diffie-Hellman 방식을 적용하고 있다. 이때 멀티캐스트 통신을 위해서 모든 멤버가 키 생성에 관여하므로, 새로운 멤버 가입 및 기존 멤버 탈퇴시 전 멤버 사이에 새로운 키를 생성해야하는 번거로움이 발생한다. 또한, Man-in the-middle attack에 의해 제 3자의 도청이 가능하다는 문제점을 안고 있다.

4.2 Iolus 방식

본 방식은 대규모 그룹을 여러 개의 소규모 그룹으로 분할하여, 멤버쉽 변동에 따른 키 변경의 영향을 줄이는 방식이다[10].

4.2.1 프로토콜

1) 시스템 계수

- GSC : Group Security Controller
- GSI : Group Security Intermediary
- GSA : Group Security Agent
- K_{GSA_MBRi} : GSA와 멤버 i사이의 비밀키
- K_{SGRP} : Subgroup을 위한 공통키
- K_{SGRP}' : Update된 Subgroup 공통키
- Sig_{MBRi} : 멤버 i의 서명
- R : 랜덤 값
- M : 메시지
- GRP_END : 멀티캐스팅 종결 확인 메시지

2) 그룹 초기화

가) GSC : Access Control List(ACL)를 작성하며, 여기에는 보안 정책관련 정보를 포함하고 있다.

나) GSI : GSI 및 그 외의 멤버는 GSC의 ACL에 맞춰 그룹에 가입하게 된다.

3) 그룹 가입

가) 참여자들은 GSA에게 그룹 가입 요구서를 안전한 유니캐스트 채널을 통해 전달한다.

나) GSA는 그룹 가입 요구서를 확인하고 비밀키 $K_{GSA-MBR}$을 생성하여, DB에 개인신상 정보와 함께 저장한다. 저장이 끝난 다음 그룹에 가입한 멤버들에게 안전한 유니캐스트 채널을 통해 $K_{GSA-MBR}$을 분배한다.

다) 기존의 Subgroup 공통키 K_{SGRP}를 K_{SGRP}'로 Update한 다음 GRP_KEY_UPDATE_JOIN 메시지를 생성하여 멤버들에게 전송한다.

- GRP_KEY_UPDATE_JOIN=$K_{SGRP}(K_{SGRP}')$

4) 그룹 재 신임

가) 그룹 가입이 수행된 다음 참여자들이 그 그룹에 지속적으로 남기를 원한다면, 안전한 유니캐스트 채널을 통해 그룹 재 신임 메시지를 전달해야 한다. 그룹 재 신임이 이뤄지면, GSA는 Network framework가 최적이 되도록 재조정한다.

5) 그룹 탈퇴

가) 그룹 탈퇴가 성립할 조건은 멤버가 Subgroup에서 탈퇴하기 위해 LEAVE 요청서를 GSA에게 전송할 경우와 GSA가 멤버를 강제 탈퇴시키려 할 경우이다.

나) 그룹 탈퇴가 발생할 경우 GSA는 K_{SGRP}를 K_{SGRP}'로 update시켜야 하며 그룹 가입 때와는 달리 다음 메시지를 생성하여, 남아 있는 멤버에게 변경된 K_{SGRP}'를 안전하게 멀티캐스트 전송한다.

- GRP_KEY_UPDATE_LEAVE
  $= K_{GSA-MBR1}(K_{SGRP}')||K_{GSA-MBR2}(K_{SGRP}')||..||K_{GSA-MBRn}(K_{SGRP}')$

6) 메시지 전송

가) 메시지 전송 유형 1

(1) 송신자는 전송 메시지(M)를 K_{SGRP}로 암호화하여 Local Subgroup에게 전송한다.

- $K_{SGRP}(M)$

(2) GSI는 전송 메시지를 복호화하여 상위 그룹의 K_{SGRP}로 암호화하여 전송하며, 동일한 방법으로 나머지 GSI는 이 정보를 받아서 복호화하고 하위 GSI에게 암호화하여 전송한다.

나) 메시지 전송 유형 2

(1) 송신자는 전송 메시지(M)를 직접 암호화하는 대신에 다음과 같이 랜덤 값(R)를 생성

하여 암호화를 수행하고, R을 K_{SGRP}로 암호화하여 연접한 다음 자신의 서명(Sig_{MBRi})을 붙여 Local Subgroup에게 전송한다.

· $Sig_{MBRi}(R(M)||K_{SGRP}(R))$

(2) GSI는 수신된 정보에 대해 인증 및 복호화 한 다음, 동일 방법으로 자신의 서명을 붙여 하위 GSI에게 전송시킴으로써 정당성을 제공한다.

(3) 메시지 전송 유형 2의 장점은 메시지 전송 유형 1에서 제공하지 못하는 메시지 신뢰성 및 무결성을 제공한다는 것이다.

7) 키 갱신

• 키 갱신은 주로 멤버 변동 시에 발생되며, 이때 키 변동을 위한 link는 이미 약속되어 있는 안전한 채널을 기초로 수행한다.

8) 멀티캐스팅 종결

• GSC는 멀티캐스팅이 안전하게 수행된 것을 확인한 다음, GRP_END 메시지를 해당 Subgroup 의 GSA에게 전송하고 이를 다시 멤버에게 전송함으로써 멀티캐스팅을 종결시킨다.
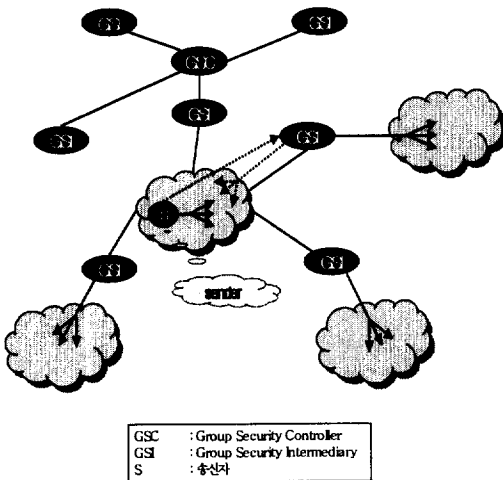
그림 1. Iolus 프로토콜의 흐름도

4.2.2 특징

본 방식은 각 멤버쉽이 Tree-Based 계층 구조로 구성된다. 각 멤버의 가입/탈퇴시 Subgroup 내에서만 키의 변경이 일어나므로, Clique 방식의 문제점을 개선하고 있다. 그러나 보안 관리 센터(GSC)의 오류 및 부정이 발생할 경우 멀티캐스트 서비스가 불가능하다. 동시에 각 Subgroup간의 통신시 중간 관리자 간에 메시지 암/복호화를 별도로 수행해야 하고, 메시지 전송 유형 2를 사용할 경우 서명 확인을 위한 별도의 공개키 관리 센터 및 암호 방식을 적용해야 하는 단점이 발생한다.

4.3 DK 방식

네트워크 환경에서 멀티캐스팅에 개체/메시지 인증, 권한 부여, 기밀성 및 무결성을 제공하고 송신자 키의 생성과 분배, 그룹으로부터 자진/강제 탈퇴의 방법을 포함하며, 멀티캐스트 트리를 통한 계층적 멀티캐스트 라우팅 알고리즘을 사용하는 방식이다[11].

4.3.1 프로토콜

1) 그룹 생성

가) 그룹 생성자

• 멤버들과 각 멤버들의 인증 리스트(authorization list)를 담고 있는 ACL(Access Control List)을 암호화하여 해당 도메인의 KDC (Key Distribution Center)에게 전달한다.

• 그룹의 특성은 SDP(Session Description Protocol)를 이용하여 기술하고 특정 주소로 SAP(Session Announcement Protocol)를 이용하여 멀티캐스팅 한다.

• 그 후 참가를 원하는 멤버들은 해당 KDC에 인증된 그룹 가입 요청 메시지(Join message)를 보내면 KDC는 ACL로부터 멤버를 인증하고 그룹 키를 갱신하다.

2) 키 관리 구조

가) GDK(Group Data Key)

• CP(Center Point)와 모든 멤버에서 공유하며, 그룹 멤버간의 교환될 패킷을 암호화하는데 사용한다.

나) DCK(Domain Control Key)

• 정당한 멤버들에게 바뀐 GDK를 전달하기 위해서 GDK를 암호화하기 위한 키로 사용된다.

다) EK(Edge Key)

• 멤버나 송신자가 멀티캐스트 트리 내에 메시지 패킷을 전송할 경우 사용자 및 메시지의

발신처를 인증하기 위해 사용된다.

라) SK(Sender Key)

• 송신자가 전송 메시지를 암호화하기 위해 사용한다.

3) 시스템 계수

• I : 그룹 생성자
• AS : 인증 서버
• $\{M\}^K$: 메시지 M을 키 K로 암호화
• MGA(Multicast Group Address) : 멀티캐스트 그룹 주소
• PK-H : H의 공개키
• SK-H : H의 개인키
• SS-H : H의 비밀키
• Permition : R-permit/ W-permit/ I-permit/ CP-permit

4) 트리 생성

가) 그룹 생성자(I)는 멤버 또는 송신자로서 그룹에 가입되도록 허가 받은 호스트들의 리스트를 준비하고 다음과 같이 메시지를 암호화하여 인증 서버(AS)에게 전달한다.

• I → AS : $\{$I-ID, MGA, CP-Address, TS, Life-Time, ACL$\}^{SK-I}$

나) AS는 전송된 메시지를 확인하고 그룹 생성에 대한 승인 여부를 점검하여 결과를 I에게 전송한다.

• AS → I : $\{$I-ID, MGA, CP-Address, TS, Life-Time, I-Permit$\}^{SK-AS}$

다) I는 수신한 그룹 생성 승인 정보를 CP에게 전달하고 멀티캐스트 그룹 생성을 요구한다. CP는 AS와 연결하여 CP의 그룹 생성 승인 정보를 획득한다.

• I → CP : $\{$I-ID, MGA, CP-Address, TS, Life-Time, I-Permit$\}^{SK-AS}$
• CP → AS : $\{$CP-ID, MGA$\}^{SK-CP}$
• AS → CP : $\{$CP-ID, MGA, TS, Life-Time, CP-Permit$\}^{SK-AS}$

라) AS는 ACL에 속한 각 호스트들의 그룹 생성 관련 정보를 만들고, 요구에 따라 분배할 수 있도록 저장한다. 각 호스트들의 그룹 생성 관련 정보는 다음과 같다.

• I → AS : $\{$I-ID, MGA, CP-Address, TS, Life-Time, ACL$\}^{SK-I}$
• H : $\{$H-ID, MGA, CP-Address, TS, Life-Time, Permit-정보$\}^{SK-AS}$
• H1 : $\{$H1-ID, MGA, CP-Address, TS, Life-Time, Permit-정보$\}^{SK-AS}$...

5) 트리 가입

가) IGMP를 사용하여 가장자리 라우터(ER)에게 가입 요청 패킷을 전송한다.

• H → ER : $\{$H-ID, MGA, Permit-Request$\}^{SK-H}$

나) 가장자리 라우터는 가장자리 키(EK)를 생성하여 순서번호(SEQ)와 같이 호스트에게 보낸다.

• ER → H : $\{\{$EK, SEQ$\}^{PK-H}\}^{SK-ER}$

다) 멤버로서 가입하는 경우와 송신자로서 가입하는 경우에 따라 각각 다르게 처리한다.

(1) 멤버로서 가입하는 경우

· ER은 AS를 통해 호스트 H의 그룹 생성 관련 정보를 수신하고, 다음과 같이 멤버 가입 요청 정보를 코어(Core)에게 전송한다.
ER → Core : $\{$Member-Join, ER-ID,MGA, Host-Join-Request$\}^{SK-ER}$

· 코어는 패킷을 점검하고 도메인 키를 변경하여 이를 그룹 내의 멤버에게 분배한 후 다음과 같은 패킷을 ER에게 보내 가입 요청을 허락한다.
Core → ER : $\{$Join-Ack, $\{\{$H-ID, MGA, DCK'$\}^{PK-H}\}^{SK-Core}\}^{SK-Core}$

· ER은 새로운 도메인 키를 새 가입자 H에게 보낸다.
ER → H : $\{\{$H-ID, MGA, DCK'$\}^{PK-H}\}^{SK-ER}$

· 코어 라우터는 CP에게 새 멤버가 가입하였음을 알리고 새로운 그룹 키가 생성 및 분배될 수 있도록 한다.
Core → CP : 새로운 멤버 가입 요청 메시지
CP : 새로운 그룹 키 GDK' 생성
CP → 모든 멤버들 : $\{\{$MGA, GDK'$\}^{SK-CP}$, CP-Capability$\}^{DCK}$

(2) 송신자로서 가입하는 경우

· ER은 자신의 코어 라우터에게 새로운 호스트가 송신자로서 가입하였음을 알린다.
ER → Core : {Sender-Join, ER-ID, H-ID,

MGA, Host-Join-Request}$^{SK-ER}$

6) 트리 탈퇴

가) 멤버 호스트의 자발적 그룹 탈퇴

(1) 호스트는 다음과 같은 메시지를 ER에게 전송한다.

· H → ER : {Leave, H-ID, MGA}$^{SK-H}$

(2) ER은 가장자리 키를 버리고 다음의 메시지를 코어 라우터에게 전달한다.

· ER → Core : {Member-Leave, ER-ID, H-ID, MGA, Host-Leave-Request}$^{SK-ER}$

(3) 코어는 저장하고 있던 H-ID, MGA, ER-ID 정보를 삭제하고 CP에게 멤버가 탈퇴하였음을 알린다. 그런 다음 CP는 새로운 그룹 키를 생성하여 모든 그룹 멤버에게 멀티캐스트한다.

· Core → CP : 그룹 탈퇴 정보

· CP : 새로운 그룹 키 GDK′ 생성

· CP → 모든 그룹 멤버 : {{DCK′}$^{SK-CP}$}^{DCK}

(4) 송신자가 그룹을 탈퇴할 때는 패킷을 ER에게 전송하고, ER은 보유하고 있던 가장자리 키를 없애고 코어에게 송신자가 탈퇴하였음을 알린다.

나) 강제 탈퇴

(1) 그룹 생성자 I가 특정 멤버 M을 그룹으로부터 방출하려고 할 때는 다음의 메시지를 그룹에게 멀티캐스트 한다.

· I → 모든 그룹 멤버 : {{Evict-Member, M-ID, MGA}$^{SK-I}$, I-Capability}^{GDK}

(2) 송신자 S가 그룹에서 추방되어야 할 때, I는 다음과 같은 메시지를 그룹 멤버들에게 멀티캐스트 한다.

· I → 모든 그룹 멤버 : {{Evict-Member, M-ID, MGA}$^{SK-I}$, I-Capability}^{GDK}

4.3.2 특 징

이 방식은 Iolus 방식에서 지적되었던, 멀티캐스트 메시지 전송시 중간 관리자 사이에 발생되는 암/복호화 과정을 줄이기 위하여 제안된 방식이다. 즉, 모든 멤버가 동일한 멀티캐스트 키를 보유함으로서, 중간 관리자의 번거로움이 해결되고 있다. 그러나 새로운 멤버 가입/탈퇴시 전 멤버의 멀티캐스트 키를 새로이 생성 및 전송해 주어야 하는 문제점이 생기고 있다.

5. 새로운 방식 제안

본 방식은 상기 제시되었던 요구 사항을 만족함과 동시에 기존의 멀티캐스트 키 관리 방식들 - Clique 방식, Iolus 방식, DK 방식- 이 안고 있던 문제점들을 해결하고 있다.

5.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술하고 있다.

- DKM_i : 도메인 키 관리자 i (i = 1, 2, 3, ... , k : k는 도메인 키 관리자 수)
- DMB_i : Domain Border i (i = 1, 2, 3, ... , k : k는 Border의 수)
- DKA_i : 도메인 키 중간 관리자 i (i = 1, 2, 3, ... , j : j는 도메인 키 중간 관리자 수)
- SGB_i : Subgroup Border i (i = 1, 2, 3, ... , j : j는 Subgroup Border의 수)
- MGB_i : Multicast Group Border i (i = 1, 2, 3, ... , k : k는 Border의 수)
- GML : 그룹 멤버 리스트
- PKM : 도메인 키 (중간)관리자들 및 각 Border의 공개키 관리자
- MBR_i : 그룹 멤버 i (i = 1, 2, 3, ... , n : n은 멤버의 수)
- R : 라우터
- GI : 그룹 초기자
- Sig_* : *의 서명
- MKey : PKM에 의해 생성된 멀티캐스트 키
- K_{PP}, K_{PS} : PKM의 공개키 및 개인키
- K_{DPi}, K_{DSi} : 각 DKM_i의 공개키 및 개인키
- K_{DAPi}, K_{DASi} : 각 DKA_i의 공개키 및 개인키
- K_{DMBPi}, K_{DMBSi} : 각 DMB_i의 공개키 및 개인키
- K_{MGBPi}, K_{MGBSi} : 각 MGB_i의 공개키 및 개인키
- K_{SGBPi}, K_{SGBSi} : 각 SGB_i의 공개키 및 개인키
- K_{D_DAi} : DKM_i와 DKA_i 사이의 공통키
- K_{MSi} : 그룹 멤버 MBR_i의 비밀키
- K_{DAi_Ms} : 각 DKA_i가 관리하는 멤버들과의 공통키
- Hdr : 메시지 전송 시 송신 그룹과 수신 그룹

의 식별 정보

- ID_* : *의 식별자
- IP_* : *의 IP 주소
- M : 멀티캐스팅 메시지

5.2 시스템 프로토콜

본 방식은 멤버쉽 가입/탈퇴 시 최소한의 키 갱신을 유도하기 위하여 각 그룹은 도메인 형식으로 분류하여 동적인 관리를 수행한다. 또한 구조적으로 제어부와 메시지 전송부로 구분함으로서 키 관리 담당자의 부담을 줄이고 메시지 전송 과정에서 발생 가능한 부정 및 오버헤드를 막고 있다. 동시에 본 방식은 인증 및 메시지 암호화를 위하여 공개키 기반구조(PKI : Public Key Infrastructure)를 적용한다. 이는 이질적인 통신망 상에서 안전하면서도 적용이 용이하여 효율성을 높이는 효과를 제공한다.

5.2.1 도메인 초기화 단계

1) DKM_i, DKA_i 및 각 Border는 안전한 유니캐스트 채널을 통해 자신의 공개키 인증서를 PKM으로부터 수신한다.
   - PKM : $Cert(ID_{DKMi}||K_{DPi}||IP_{DKMi}) \rightarrow DKM_i$
     : $Cert(ID_{DKAi}||K_{DAPi}||IP_{DKAi}) \rightarrow DKA_i$
     : $Cert(ID_{MGBi}||K_{MGBPi}||IP_{MGBi}) \rightarrow MGB_i$
     : $Cert(ID_{DMBi}||K_{DMBPi}||IP_{DMBi}) \rightarrow DMB_i$
     : $Cert(ID_{SGBi}||K_{SGBPi}||IP_{SGBi}) \rightarrow SGB_i$
2) 각 도메인은 DKM_i를 정점으로 멤버들을 분할하여 담당하는 각 DKA_i를 계층적으로 관리한다. 공개키 인증서 수신이 끝나게 되면 도메인 상의 각 관리자들은 상호 인증을 수행한다.

5.2.2 그룹 초기화 단계

1) GI는 그룹 멤버 리스트(GML)를 작성하여 자신의 식별자 ID_{GI}와 함께 서명을 수행하여 PKM에게 전송한다.
   - GI : $Sig_{GI}(ID_{GI}||GML) \rightarrow PKM$
     : $GML = (ID_{MBR1}||\cdots||ID_{MBRn})$
2) PKM은 서명 확인을 통해 GI 및 GML을 인증하고 멀티캐스트 서비스를 위한 MKey를 생성한다. 단, MKey는 그룹이 형성될 때, 오직 관련된 Border들(SGB_i, DMB_i, MGB_i)에게만 제공함으로서 신뢰성을 높이고 있다.
   - PKM : $K_{BPi}(MKey||Sig_{PKM}(ID_{PKM})) \rightarrow$ 각 Border (SGB_i, DMB_i, MGB_i)
     : $K_{BPi} \in \{K_{SGBPi}, K_{DMBPi}, K_{MGBPi}\}$
3) PKM은 해당 Domain에게 공개키를 이용하여 안전하게 GML을 전송한다.
   - PKM : $K_{DPi}(GML||Sig_{PKM}(GML)) \rightarrow DKM_i$

5.2.3 그룹 멤버 가입 단계

1) DKM_i는 도메인 내에서 DKA_i와의 통신 시 사용할 K_{D_DAi}를 생성하여 유니캐스트 채널을 통하여 안전하게 DKA_i에게 전송한다.
   - DKM_i : $K_{DAPi}(K_{D_DAi}||Sig_{PKM}(K_{D_DAi})) \rightarrow DKA_i$
2) 그룹에 멤버로 가입할 사용자들은 자신의 서명을 이용하여 DKA_i에게 자신을 인증하고 자신의 비밀키 K_{MSi}를 K_{DAPi}로 암호화하여 안전하게 전송한다.
   - MBR_i : $K_{DAPi}(K_{MSi}||Sig_{Mi}(ID_{MBRi}||K_{MSi})) \rightarrow DKA_i$
3) DKA_i는 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 다음과 같이 그룹 가입 멤버 리스트를 생성해 DKM_i에게 전송한다.
   - DKA_i : $K_{D_DAi}(Sig_{DKAi}(ID_{MBR1}||\cdots||ID_{MBRi})) \rightarrow DKM_i$
4) DKM_i는 각 DKA_i로부터 수신된 그룹 가입 멤버 리스트에 대해 복호 및 인증을 수행한 다음 GML과 비교 확인한다.
5) DKA_i는 수신된 비밀키 K_{MSi}를 이용하여 각 멤버에게 K_{DAi_Ms}를 안전하게 전송해 준다. 동시에 이 K_{DAi_Ms}는 DKM_i 및 SGB_i에게 안전하게 전송된다.
   - DKA_i : $K_{MSi}(K_{DAi_Ms}) \rightarrow MBR_i$
     : $K_{D_DAi}(K_{DAi_Ms}) \rightarrow DKM_i$
     : $K_{SGBPi}(K_{DAi_Ms}) \rightarrow SGB_i$

5.2.4 멀티캐스트 메시지 전송 단계

메시지 전송 단계는 멀티캐스트 메시지 전송부로서 오직 멤버들 MBR_i와 각 Border들만이 관여한다. 이 단계는 도메인 내 각 멤버들에게 메시지를 전송하는 내부 전송 과정과 타 도메인 및 다른 멀티캐스트 그룹에 속한 멤버들에게 보내는 외부 전송 과정으로

분류된다.

1) 내부 전송 과정

가) 도메인 전체 전송

(1) 각 멤버들은 K_{DAi_Ms}를 이용하여 멀티캐스트 메시지 M을 암호화한 다음 SGB_i에게 전송한다.

- MBR_i : $K_{DAi_Ms}(M) \rightarrow SGB_i$

(2) SGB_i는 수신된 정보를 복호화하고, 멀티캐스트 메시지 M을 MKey로 암호화하여 각 SGB_i'에게 전송한다.

- SGB_i : $K_{DAi_Ms}(K_{DAi_Ms}(M)) = M$
- SGB_i : $Mkey(M) \rightarrow SGB_i'$
  : $SGB_i \neq SGB_i'$

(3) 각 SGB_i는 수신된 정보를 복호화하고 이를 자신이 속한 그룹의 공통키로 암호화하여 그룹 멤버들에게 전송한다.

- SGB_i : $MKey(MKey(M)) = M$
  : $K_{DAi_Ms}'(M) \rightarrow MBR_i'$
  : K_{DAi_Ms}'는 DKA_i'와 그 Subgroup에 속한 멤버들간의 공통키
  : $MBR_i \neq MBR_i'$

(4) 각 Subgroup의 멤버 MBR_i'는 K_{DAi_Ms}'로 수신된 정보를 복호화하여 메시지를 확인한다.

- MBR_i': $K_{DAi_Ms}'(K_{DAi_Ms}'(M)) = M$

나) 특정 Subgroup 전송

(1) 각 멤버들은 K_{DAi_Ms}를 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB_i에게 전송한다.

- MBR_i : $K_{DAi_Ms}(Hdr||M) \rightarrow SGB_i$

(2) SGB_i는 암호화되어 수신된 정보를 복호화한다.

- SGB_i : $K_{DAi_Ms}(K_{DAi_Ms}(Hdr||M)) = Hdr||M$

(3) SGB_i는 Hdr을 확인하고 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 자신의 서명과 함께 SGB_{i+1}에게 전송한다.

- SGB_i : $(Hdr||Sig_{SGBi}(Hdr)||MKey(M)) \rightarrow SGB_{i+1}$

(4) 해당 SGB_{i+1}는 Hdr과 서명을 확인하고 수신된 정보를 복호화한다. 복호된 멀티캐스트 메시지 M을 자신이 속한 Subgroup 공통키로 암호화하여 Subgroup 멤버들에게 전송한다.

- SGB_{i+1} : Hdr, $Sig_{SGBi}(Hdr)$ 확인
  : $MKey(MKey(M)) = M$
  : $K_{DAi+1_Ms}(M) \rightarrow MBR_{i+1}$
  : K_{DAi+1_Ms}는 DKA_{i+1}과 그 Subgroup에 속한 멤버들간의 공통키

(5) Subgroup의 멤버 MBR_{i+1}은 K_{DAi+1_Ms}로 수신된 정보를 복호화하여 메시지를 확인한다.

- MBR_{i+1}: $K_{DAi+1_Ms}(K_{DAi+1_Ms}(M)) = M$

2) 외부 전송 과정

가) 도메인에서 도메인으로의 전송

(1) 각 멤버들은 K_{DAi_Ms}를 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB_i에게 전송한다.

- MBR_i : $K_{DAi_Ms}(Hdr||M) \rightarrow SGB_i$

(2) SGB_i는 암호화되어 수신된 정보를 복호화한 후에 Hdr을 확인하고 자신의 서명과 함께 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 DMB_i에게 전송한다.

- SGB_i : $K_{DAi_Ms}(K_{DAi_Ms}(Hdr||M)) = Hdr||M$
  : $(Hdr||Sig_{SGBi}(Hdr)||MKey(M)) \rightarrow DMB_i$

(3) DMB_i는 Hdr을 확인하고 인접 도메인 Border DMB_{i+1}에게 전송한다.

- DMB_i : $(Hdr||Sig_{SGBi}(Hdr)||MKey(M)) \rightarrow DMB_{i+1}$

(4) DMB_{i+1}은 Hdr과 서명을 확인하고 해당 도메인에 속한 모든 SGB_{i+1}에게 전송한다.

- DMB_{i+1} : $MKey(M) \rightarrow SGB_{i+1}$

(5) 전송된 메시지는 각 SGB_{i+1}에 의해 복호화된 다음 각 그룹의 모든 멤버들에게 암호화되어 전송된다.

- SGB_{i+1} : $Mkey(MKey(M)) = M$
  : $K_{DAi+1_Ms}(M) \rightarrow MBR_{i+1}$
  : K_{DAi+1_Ms}는 DKA_{i+1}와 그 Subgroup에 속한 멤버들간의 공통키

(6) 각 DKA_{i+1}에 속한 Subgroup의 모든 멤버 MBR_{i+1}은 K_{DAi+1_Ms}로 복호화하여 메시지를 확인한다.

- MBR_{i+1}: $K_{DAi+1_Ms}(K_{DAi+1_Ms}(M)) = M$

나) 멀티캐스트 그룹간 메시지 전송

멀티캐스트 그룹간 메시지 전송 시에는 PKM과 연결되어 있는 MGB_i를 통해 이루어지며, 모든 전송과

정은 도메인에서 도메인으로의 전송과정과 동일하다.

(1) 각 멤버들은 K_{DAi_Ms}를 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB_i에게 전송한다.

· MBR_i : $K_{DAi_Ms}(Hdr||M) \rightarrow SGB_i$

(2) SGB_i는 암호화되어 수신된 정보를 복호화한 후에 Hdr을 확인하고 자신의 서명과 함께 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 DMB_i에게 전송한다.

· SGB_i : $K_{DAi_Ms}(K_{DAi_Ms}(Hdr||M))$ = Hdr||M : $(Hdr||Sig_{SGBi}(Hdr)||MKey(M)) \rightarrow DMB_i$

(3) DMB_i는 Hdr을 확인하고 MGB_i에게 전송한다.

· DMB_i : $(Hdr||Sig_{SGBi}(Hdr)||MKey(M)) \rightarrow MGB_i$

(4) MGB_i는 Hdr을 확인하고 MGB_{i+1}에게 전송한다.

· MGB_i : $(Hdr||Sig_{SGBi}(Hdr)||MKey(M)) \rightarrow MGB_{i+1}$

(5) MGB_{i+1}은 Hdr과 서명을 확인하고 해당 멀티캐스트 그룹에 속한 모든 DMB_{i+1}에게 전송한다.

· MGB_{i+1}: $MKey(M) \rightarrow DMB_{i+1}$

(6) 전송된 메시지는 각 DMB_{i+1} 에 의해 해당 도메인의 모든 SGB_{i+1}에게 전송된다.

· DMB_{i+1}: $MKey(M) \rightarrow SGB_{i+1}$

(7) 전송된 메시지는 각 SGB_{i+1}에 의해 복호화된 다음 각 그룹의 모든 멤버들에게 암호화되어 전송된다.

· SGB_{i+1} : Mkey(MKey(M)) = M
: $K_{DAi+1_Ms}(M) \rightarrow MBR_{i+1}$
: K_{DAi+1_Ms}는 DKA_{i+1}와 그 Subgroup에 속한 멤버들간의 공통키

(8) 각 DKA_{i+1}에 속한 Subgroup의 모든 멤버 MBR_{i+1}은 K_{DAi+1_Ms}로 복호화하여 메시지를 확인한다.

· MBR_{i+1}: $K_{DAi+1_Ms}(K_{DAi+1_Ms}(M))$ = M

5.2.5 신규 멤버 가입 및 기존 멤버 탈퇴 단계

1) 신규 멤버 가입

신규 멤버 가입은 다음과 같은 과정을 통해 수행된다.

가) 그룹에 신규 멤버로 가입할 사용자들은 자신의 서명을 이용하여 DKA_i에게 자신을 인증하고 자신의 비밀키 K_{MSi}'를 K_{DAPi}로 암호화하여 안전하게 전송한다.

• MBR_i': $K_{DAPi}(K_{MSi}'||Sig_{Mi}(ADD||ID_{MBRi}')||K_{MSi}')) \rightarrow DKA_i$
: ADD는 신규 가입 대상자임을 나타내는 식별자

나) DKA_i는 신규 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 다음과 같이 신규 가입 멤버 정보를 생성해 DKM_i에게 전송한다.

• DKA_i : $K_{D_DAi}(Sig_{DKAi}(ADD||ID_{MBRi}')) \rightarrow DKM_i$

다) DKM_i는 DKA_i로부터 수신된 그룹 신규 가입 멤버 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML′을 PKM에게 전송한다.

• DKM_i : GML → GML′
: GML′ = $(ID_{MBR1}||\cdots||ID_{MBRn}||ID_{MBRi}')$
: $K_{DPi}(Sig_{DKMi}(GML')) \rightarrow$ PKM

라) PKM은 GML′의 수정 내용을 확인한 다음 GML을 GML′으로 교체한다.

마) DKA_i는 수신된 비밀키 K_{MSi}'를 이용하여 신규 가입 멤버에게 K_{DAi_Ms}를 안전하게 전송해 준다. 신규 멤버 가입시에는 K_{DAi_Ms}에 대한 별도의 변화는 필요 없게 된다.

• DKA_i : $K_{MSi}'(K_{DAi_Ms}) \rightarrow MBR_i'$

2) 기존 멤버 탈퇴

기존 멤버 탈퇴 시에는 신규 멤버 가입 때와는 다르게 남아 있는 멤버들을 위해 기존의 K_{DAi_Ms}를 갱신하여 분배한다. 이를 통해 그룹 탈퇴자로부터 기존 멤버들에 대한 보안성을 획득할 수 있다.

가) 그룹 탈퇴를 희망하는 멤버는 다음과 같은 정보를 생성하여 DKA_i에게 안전하게 전송한다.

• MBR_i : $K_{DAPi}(Sig_{Mi}(DEL||ID_{MBRi})) \rightarrow DKA_i$
: DEL은 그룹 탈퇴 희망자임을 나타내는 식별자

나) 기존의 멤버 MBR_i가 탈퇴할 경우 DKA_i는 다음과 같이 탈퇴 멤버 정보를 생성해 DKM_i에게 전송한다.

- $DKA_i : K_{D_DAi}(Sig_{DKAi}(DEL||ID_{MBRi})) \rightarrow DKM_i$

다) DKM_i는 DKA_i로부터 수신된 그룹 탈퇴 멤버 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML'을 안전하게 PKM에게 전송한다.

- DKM_i : GML → GML'
  : $GML' = (ID_{MBR1}||\cdots||ID_{MBRi-1}||ID_{MBRi+1}||\cdots||ID_{MBRn})$
  : $K_{DPi}(Sig_{DKMi}(GML')) \rightarrow PKM$

라) PKM은 GML'의 수정 내용을 확인한 다음 GML을 GML'으로 교체한다.

마) DKA_i는 새로운 공통키 K_{DAi_Ms}'를 생성하여 남아 있는 기존의 멤버들 MBR_i', DKM_i 및 SGB_i에게 안전하게 전송한다.

- DKA_i : $K_{DAi_Ms} \rightarrow K_{DAi_Ms}'$
  : $K_{MSi}(K_{DAi_Ms}') \rightarrow MBR_i'$
  : MBR_i'는 탈퇴 멤버를 제외한 기존 멤버
  : $K_{D_DAi}(K_{DAi_Ms}') \rightarrow DKM_i$
  : $K_{SGBPi}(K_{DAi_Ms}') \rightarrow SGB_i$

5.2.6 그룹 합병 및 그룹 분할

1) 그룹 합병

기존 두 그룹의 합병은 다음과 같은 과정을 통해 수행된다.

가) 그룹 합병을 원하는 DKA_i는 그룹 합병 요구 메시지를 다음과 같이 통고한다.

- DKA_j : $Hdr||K_{DAj_Ms}(Request) \rightarrow SGB_j$
- SGB_j : $Hdr||Sig_{SGBi}(Hdr)||MKey(Request) \rightarrow SGB_i$
- SGB_i : $K_{DAi_Ms}(Request) \rightarrow DKA_i$

나) DKA_i는 Border를 통해 받은 전송 정보를 복호화하여 확인하고 그룹 합병을 결정한다. 그룹 합병이 결정되면 그룹 합병 승인 메시지를 DKA_j에게 전송한다.

다) 승인 메시지를 받은 DKA_j는 그룹 멤버 리스트 GML_j를 DKA_i에게 전송한다.

라) DKA_i는 새로운 공통키 K_{DAi+j_Ms}를 생성하여 DKM_i에게 그룹 합병 정보와 새로운 공통키 K_{DAi+j_Ms} 및 DKA_j의 그룹 멤버 리스트 GML_j를 함께 전송한다.

- $DKA_i : K_{D_DAi}(Sig_{DKAi}(Union||GML_j||K_{DAi+j_Ms})) \rightarrow DKM_i$
  : Union은 그룹 합병 정보 식별자

마) DKM_i는 DKA_i로부터 수신된 그룹 합병 정보에 대해 복호 및 인증을 수행한 다음 새로운 그룹 멤버 리스트 GML_{i+j}를 생성하여 PKM에게 전송한다.

- DKM_i : GML_{i+j}
  : $GML_{i+j} = (GML_i+GML_j)$
  : $K_{DPi}(Sig_{DKMi}(GML_{i+j})) \rightarrow PKM$

바) DKA_i는 새로운 공통키 K_{DAi+j_Ms}를 모든 멤버들 MBR_i와 SGB_i에게 DKA_i와 모든 멤버들 사이의 공통키로 암호화하여 전송하고 DKA_j에게는 새로운 공통키 K_{DAi+j_Ms} 및 DKA_i의 그룹 멤버 리스트 GML_i를 함께 전송한다.

- DKA_i : $K_{BPi}(K_{DAi+j_Ms}) \rightarrow SGB_i$
  : $K_{DAi_Ms}(K_{DAi+j_Ms}) \rightarrow MBR_i$
  : $Hdr||K_{DAj_Ms}(GML_i||K_{DAi+j_Ms}) \rightarrow DKA_j$

사) DKA_j는 새로운 공통키 K_{DAi+j_Ms}를 모든 멤버들 MBR_j와 SGB_j에게 DKA_j와 모든 멤버들 사이의 공통키로 암호화하여 전송하고 DKM_j에게는 DKA_i의 그룹 멤버 리스트 GML_i를 그룹 합병 정보와 함께 전송한다.

- DKA_j : $K_{BPj}(K_{DAi+j_Ms}) \rightarrow SGB_j$
  : $K_{DAj_Ms}(K_{DAi+j_Ms}) \rightarrow MBR_j$
  : $K_{D_DAj}(Sig_{DKAj}(Union||GML_i||K_{DAi+j_Ms})) \rightarrow DKM_j$
  : Union은 그룹 합병 정보 식별자

아) DKM_j는 DKA_j로부터 수신된 그룹 합병 정보에 대해 복호 및 인증을 수행한 다음 새로운 그룹 멤버 리스트 GML_{i+j}를 생성한다.

- DKM_j : GML_{i+j}
  : $GML_{i+j} = (GML_i+GML_j)$

2) 그룹 분할

가) 합병된 그룹에서의 그룹 분할

그룹의 분할은 그룹 합병과는 달리 그룹 분할 정보를 DKA_{i+j}, DKM_{i+j}, SBG_{i+j}, 모든 그룹 멤버 MBR_{i+j}에게 전달하고 이를 전달받은 각 개체는 해당 그룹키를 삭제한다. 또한 DKM_{i+j}와 PKM_{i+j}는 그룹의 멤버 리스트 GML_{i+j}를 삭제함으로써 완료된다.

나) 기존 그룹에서의 그룹 분할

기존 그룹DKA_i가 분할될 경우 새로 생성되는 그

룹의 DKA_j와 SGM_j가 생성되며, 각 그룹은 다음과 같은 과정으로 새로운 GML과 그룹 키를 생성한다.

(1) 기존 그룹의 DKA_i는 5.2.5의 기존 멤버 탈퇴 시와 같은 방식으로 GML과 그룹 키를 갱신한다.

(2) 새로 생성된 그룹의 DKA_j는 5.2.3의 그룹 멤버 가입단계와 같은 과정을 수행한다.

그림 2. 제안된 멀티캐스트 키 관리 구조도

5.3 새로운 방식의 특징

본 제안 방식은 다음과 같은 특징을 가지고 있다.

1) Clique 방식의 문제점 해결

새로운 멤버 가입 및 기존 멤버 탈퇴 시 모든 멤버에게 새로운 키를 생성 및 분배하는 문제점을 해결하였고, 멤버를 도메인 상의 Subgroup으로 나누는 기법을 적용함으로서 그룹 멤버 탈퇴가 발생하는 Subgroup의 K_{DAi_Ms}만 갱신하면 된다.

2) Iolus 방식의 문제점 해결

도메인 관리를 위한 제어부와 메시지 전송을 위한 메시지 전송부로 구분함으로서 메시지 전송시 중간 과정에서 노출되는 것을 막는다. 또 GSC의 오류 및 부정에 대한 해결 방안 제시 - Iolus 방식은 집중형 Tree Based 구조를 가지고 있으므로 최상위 노드의 오류에 대해 멤버 전체의 통신 단절을 가져 올 수 있다는 문제점이 발생하고 있다. 그러나 본 방식은 각 Subgroup을 그물형 도메인 내에 계층적으로 분포시킴과 동시에 오류에 대한 새로운 path를 지정함으로서 이 문제를 해결하고 있다.

3) DK 방식의 문제점 해결

DK 방식은 Iolus에서 문제가 되고 있는 중간 관리자의 메시지 암/복호화의 문제점을 해결하기 위해 각 멤버가 그룹 키를 가지게 하고 있다. 그러나, 이 방식은 새로운 멤버 가입 또는 기존 멤버 탈퇴 시 모든 멤버에게 새로운 그룹 키를 전송해야하는 문제점을 가지고 있다. 이에 대해 본 방식은 멤버 탈퇴 시 Subgroup의 K_{DAi_Ms}만 변경하면 되므로 DK 방식의 문제점을 해결하고 있다.

4) 기타 (PKI(Public Key Infrastructure))

본 방식은 그 구조에 있어 공개키 기반구조와 유사한 점을 가지고 있다. 현재 공개키 기반구조 구축이 진행 중에 있으며, 향후 본 방식을 공개키 기반구조에 적용했을 경우 별도의 기반구조 구축 없이 멀티캐스트 그룹 키 분배가 가능함으로 상호간의 이식성이 뛰어날 뿐만 아니라 기반구조 구축을 위한 추가 비용을 줄일 수 있다. 또한 본 방식은 도메인 Subgroup으로 나누어져 있어 동적으로 그룹을 생성할 수 있도록 확장성을 제공한다.

마지막으로 그룹 키 분배를 위한 전체 멀티캐스트 그룹내의 통신량과 연산량에 있어 다른 방식에 비해 효율적이다. 이와 관련한 자세한 내용은 6.2에서 설명하기로 한다.

6. 각 방식별 비교 분석

다음은 멀티캐스트 키 관리 구조 요구 사항에 기초하여 기존 방식과 제안 방식을 비교 분석한 결과이다.

6.1 각 방식별 안전성 비교 분석

1) Clique 방식

참가자의 증가에 따른 암호 키의 수 및 중계 라우터에서의 키의 양은 증가하지 않으며, n-1번의 통신을 통해 비밀키를 얻을 수 있어 정적인 키 분배의 경우에 적합하고 병목현상이 발생하지 않는다. 그러나 신규 멤버 가입 및 기존 멤버 탈퇴 시 그룹 관리자는 O(n)의 메시지 교환을 수행해야 하며, 그룹의 규모가 커질 경우 그 메시지가 기하급수적으로 늘어나

확장성이 떨어져 효율적이지 못하다.

2) Iolus방식

기존 멤버의 탈퇴나 새로운 멤버가 가입할 경우 그 멤버가 속한 그룹의 키만 변경하게 되므로 그룹 키 갱신에 드는 비용을 줄일 수 있다. 그러나 그룹 멤버가 증가하게 되면 GSA에서 키의 양이 증가하게 되며, 서브그룹 사이에서의 메시지 전송 시 GSI에서는 암호/복호에 따른 전송지연이 발생하게 된다. 또한 중계과정에서 고장이 발생하면 지연이 발생된다는 단점을 가지고 있다.

3) DK 방식

본 방식은 상호 인증과 메시지 무결성을 보장하기 위해 메시지 생성시 서명을 수행하여 전송하고 이를 확인하게 된다. 또한, 권한 허가서를 제공하여 범위의 한정을 주고 융통성을 제공하고 있으나, 멤버 가입 단계에 있어 각 단계별로 서명 및 암/복호가 이뤄지게 되므로 타 방식에 비해 사용되는 암호 키의 수가 증가하고 있다. 멤버 변동이 있을 경우 새로운 그룹 키를 만들어 모든 멤버에게 전송하게 되는데 이 그룹 키를 생성하기 위한 프로토콜 명시가 없다.

4) 제안 방식

제안 방식에서는 기존 방식들에서 나타나고 있는 멤버 가입/탈퇴 시 새로운 그룹 키를 생성하여 남아있는 멤버들에게 분배해야 하는 문제점을 도메인 상의 Subgroup으로 나누는 기법을 이용하여 해결하고 있다. 동시에 본 방식에서는 Border에 의해 각 1번의 암/복호화 과정을 통해 메시지를 전달하므로 효율성을 높이고 있다.

6.2 각 방식별 그룹 키 분배 방식에 따른 통신량 비교 분석

다음은 각 방식을 그룹 키 분배 방식에 적용했을 때 그룹 키를 분배하기 위한 전체 통신량을 계산하여 비교 분석한 결과이다.

기존 KDC를 이용할 경우 KDC는 각각의 멤버들

표 1. 각 멀티캐스트 키 관리 방식별 비교 분석

항목 \ 대상	기존 KDC	Clique	Iolus	DK	제안방식
메시지 암호키의 수	n-1	3	3	7	3
암호 방식 (대칭, 비대칭)	(O,O)	(O,O)	(O,O)	(O,O)	(O,O)
참가자 증가에 따른 키 증가	X	X	X	X	X
탈퇴자에 대한 참가자 보안성	O	O	O	O	O
새로운 참가자에 대한 이전 트래픽 보안성	O	O	O	O	O
참가자 수에 따른 중계 라우터 키의 양	증가	변화 없음	증가	증가	변화 없음
기반 구조	Tree 구조	any	Ring 구조	CBT	도메인 SubTree
참여개체수	2	2	4	3	4
상호 인증성	O	O	O	O	O
통신횟수	n	2(n-1)	js+j	js+j	js
통신 신뢰성	X	X	X	O	O
병목현상 극복	O	O	X	O	O
무결성	O	X	X	O	O
키 갱신 범위	ALL	ALL	Sub-Group	ALL	Sub-Group
메시지 전송시 암/복호화 횟수	n	1	j	1	2

k : 도메인 수, j : 중간 관리자(중계 라우터) 수, n : 멤버

과 비밀키를 공유하고 있으며, 그룹 키를 생성하고 분배한다. 이 그룹 키를 분배하기 위해서는 각 멤버들과 통신하게 되므로 n번의 통신을 하게 된다. n은 그룹 멤버의 수이다.

Clique 방식은 버스형 또는 링형 구조로서 그룹 키 생성을 위해 그룹 키 생성 정보 전송을 위해 n-1번의 통신을 하며, 그룹 키 전송을 위해 다시 n-1번의 통신을 한다. 따라서 그룹 키 분배를 위해 2(n-1)번의 통신회수를 갖게된다. Iolus 방식의 경우 각 그룹 멤버들을 소규모의 Subgroup으로 나누어 관리하는 방식으로 키 분배를 위해 GSC(Group Security Controller)와 Subgroup사이의 통신이 필요하며, Subgroup과 멤버 사이의 통신이 필요하다. 따라서 Subgroup 관리자를 j라하고 멤버를 s라 할 때 그룹 키 분배를 위한 통신회수는 js+j가 된다.

DK 방식은 Iolus와 같은 구조를 갖고 있으며, 다른 점은 라우터에서 발생하는 암/복호화에 따른 오버헤드를 줄인 것이다. 따라서 이 구조를 그룹 키 분배 방식에 적용할 경우 Iolus와 같은 통신회수를 갖는다. j는 라우터 수이고 n은 멤버의 수이다.

마지막으로 본 제안 방식에서는 각 그룹 멤버들을 도메인 상의 Subgroup으로 나누는 기법을 이용하고 있다. 동시에 그룹 멤버 관련 키 생성 시 오직 중간 키 관리자만이 관여하므로 js의 통신회수를 갖는다.

아래 표 2는 각 적용 방식별 통신량을 보여주고 있다. 각 그룹 키 분배 방식에 있어서의 통신량을 각 구조에 적용했을 때 동일하게 나오고 있으나 BD방식은 각 구조에 따라 다른 것을 볼 수 있다. 이것은 중계 라우터가 있는 방식에서는 라우터에서 사용자 확인을 위한 통신이 필요하지만 중계 라우터가 없는 방식과 중계 라우터가 있더라도 사용자 확인을 하지 않는 방식에서는 이러한 통신이 없기 때문에 통신량이 다르게 나오고 있다. 각 적용 방식별 통신량은 표에서 나타나 있듯 각 구조에 Diffie-Hellman 방식과 제안 방식인 PL 방식을 적용했을 때 다른 방식들에 비해 좋은 것으로 나타나고 있다. 그러나 앞 절에서 언급했듯이 Diffie-Hellman 방식은 안전성과 보안성 및 멤버의 가입 탈퇴에 따른 그룹 키 재분배의 문제점을 가지고 있다. 반면 제안 방식은 각 구조에서 나타난 문제점들을 해결하고 있으며, 멀티캐스팅 키 분배를 위한 요구 사항들을 만족하고 있기 때문에 안전성과 효율성 측면에서 좋다고 할 수 있다. 또한, 제안 구조에 PL 방식을 적용했을 때 안전성을 보장하면서 다른 방식들에 비해 최적의 통신량을 보이고 있다.

6.3 각 방식별 키 분배 방식에 따른 연산량 비교 분석

각 구조를 그룹 키 분배 방식에 적용했을 경우 사용자 측면에서의 연산량을 구하여 비교 분석해 본다. 먼저 각 키 분배 방식에 따른 지수승(Exponential) 연산량을 구해보면 다음과 같다.

- U=2k : Diffie-Hellman 방식의 Exponential 연산량
- W=nc : ITW 방식의 Exponential 연산량
- X=ck(3+n)+6c : KO 방식의 Exponential 연산량
- Y=c(2n+4) : BD 방식의 Exponential 연산량
- Z=c(n+2)+k(c+1) : 제안(PL) 방식의 Exponential 연산량

여기서 c는 상수이고 k는 키 크기이다. 각 방식의 Exponential 연산량은 키 분배에 참여하는 멤버와 라우터에서 계산되어 지는 연산량이므로 각 방식별 키 분배 방식에 따른 연산량을 구해보면 다음 표 3과 같다. 여기서 중계 라우터간의 키 분배에 있어 사용되어 지는 키가 불확실하며, 사용자 측면에서의 연산

표 2. 각 적용 방식별 통신량 비교

구조 \ 방식	Diffie-Hellman	ITW 방식	KO 방식	BD 방식	PL 방식
기존 KDC	2n	5n	3n	4n	2n
Clique	2(n-1)	5(n-1)	3(n-1)	4(n-1)	2(n-1)
Iolus	2(js+j)	5(js+j)	3(js+j)	5(js+j)	2(js+j)
DK	2(j+n)	5(j+n)	3(j+n)	3(j+n)	2(j+n)
제안방식	2js	5js	3js	5js	2js

k:도메인 수, j:중간 관리자(중계 라우터) 수, s:subguoup 멤버 수, n:그룹 멤버들의 수

표 3. 각 적용 방식별 연산량 비교

구조 \ 방식	Diffie-Hellman	ITW 방식	KO 방식	BD 방식	PL 방식
기존 KDC	U(n)	W(n)	X(n)	Y(n)	Z(n)
Clique	U(n)	W(n)	X(n)	Y(n)	Z(n)
Iolus	U(js)	W(js)	X(js)	Y(js)	Z(js)
DK	U(n)	W(n)	X(n)	Y(n)	Z(n)
제안방식	U(js)	W(js)	X(js)	Y(js)	Z(js)

k : 도메인 수, j : 중간 관리자(중계 라우터) 수, s: sub-guoup 멤버 수, n:그룹 멤버들의 수

량을 살펴보기 때문에 라우터간의 키 분배 연산량은 고려하지 않는다.

위의 표에서 보면 n은 그룹 멤버들의 수이고 js는 라우터와 Subgroup의 멤버 수이므로 n과 js는 차이가 없다고 볼 수 있으며, Exponential 연산량 비교에서 Diffie-Hellman 방식과 ITW 방식이 효과적이다. 그러나 앞 절에서 언급했듯이 이 방식들은 안전성이나 효율성 및 멤버 가입/탈퇴에 따른 그룹 키 재분배에 있어 문제점을 내재하고 있다. 따라서 그 외의 다른 방식들을 고려해 볼 때 제안 방식이 가장 효율적이다.

7. 결 론

현대 사회는 정보 통신 분야의 발전과 더불어 다양한 멀티캐스트 관련 서비스 요구가 증대되고 있다. 그러나 멀티캐스트 서비스는 기본적으로 다자간 통신을 요구함으로서 안전성, 효율성 및 확장성 부분에서 취약성을 드러내고 있다.

본 논문에서는 이러한 취약성을 극복하기 위해 필요한 요구 사항을 살펴보았고, 기존의 멀티캐스트 키 관리 구조들이 이에 어떻게 대처하는지 고찰하였다. 또한 기존의 그룹 키 분배 방식들을 고려하여, 이러한 요구 사항 및 기존 방식의 문제점을 해결할 수 있는 새로운 멀티캐스트 키 관리 구조를 제안하여 기존의 방식들과 안전성, 효율성 및 확장성 부분에서 비교 분석하였다.

이를 통해 제안된 방식은 기존의 방식들에 비해 안전성과 확장성을 제공하면서 통신량과 연산량 측면에서 효율적인 구조로 이루어져 있음을 확인하였다. 따라서 본 방식은 향후 더욱 다양해지는 멀티캐스트 관련 서비스 분야에서 적극적으로 대처할 수 있으리라 기대된다.

참 고 문 헌

[1] W. Diffie and M. Hellan, "New Direction in cryptography," IEEE Trans., It-22, pp.644-654, 1976.

[2] I. Ingemarsson, D. Tang and C. Wong, "A Conference key distribution system," IEEE Trans., It-28, pp. 714-720, 1982.

[3] K. Koyama and K. Ohta, "Identity-based conference key distribution systems," Proceedings of Crypto '87, lecture Notes in Computer Science no. 293, Springer-Verlag, pp.175-184, 1988.

[4] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution Systems," EUROCRYPT '94, pp. 279-290, 1994.

[5] Y. Yacobi, "Attack on the Koyama-Ohta Identity-based key distribution systems," Proceedings of Cryto'87, Lecture Notes in Computer Science no. 293, Springer-Verlag, pp. 429-433, 1988.

[6] E. Brickell, P. Lee and Y. Yacobi, "Secure Audio teleconference," Advances in Cryptology-Crypto '87, Lecture Notes in Computer Science 293, pp. 418-426, 1988.

[7] 박희운, 이임영, "효율적인 회의용 키 분배 방식에 관한 연구," 한국통신정보보호학회 충청지부, 1999

[8] M. Steiner, G. Tsudik and M. Waidner, "Diffie-Hellman Key distribution extended to group," In ACM Symposium on Computer and Communication Security, 1996.

[9] G. Caronni, M. Walldvogel and D. Plattner, "Efficient Security for Large Dynamic Multicast Groups," WETIC '98, 1998.

[10] S. Mittra, "Iolus : A Framework for Scalable Secure Multicasting," 1997.

[11] "멀티캐스트를 위한 키 분배 메커니즘 설계 및 구현" ETRI 최종 보고서, 1999.

[12] A. Ballardie, "Scalable Multicast Key distribution," RFC1949, May, 1996.
[13] A. Ballardie, "Core Based Tree(CBT) Multicast Routing Architecture," Request for Comments 2201, Internet Activities Board, Oct, 1997.
[14] T. Maufer and C. Semeria, "Introduction to IP Multicast Routing," draftietf-mboned-intro-multicast-00.txt, Mar, 1997.
[15] J. Moyer, R. Rao and P. Rohatgi, "A Survery of Security Issues in Multicast Communications," IEEE Network, Nov/Dec, 1999.
[16] T. Hardjono, B.Cain and N. Doraswamy, "A Framework for Group key Management for Multicast Security," draftietf-ipsec-gkmframework-02.txt, Feb, 2000.

박 희 운

1997년 2월 순천향대학교 컴퓨터 공학부 졸업
1999년 2월 순천향대학교 전산학 전공 석사
1999년 3월~현재 순천향대학교 전산학전공 박사과정
관심분야 : 암호이론, 컴퓨터 보안

이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학 전공 석사
1989년 3월 오사카대학 통신공학 전공 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안